Title (en)

APPARATUS AND METHOD FOR PRODUCING AN ASYMMETRIC CHECKSUM

Title (de)

VORRICHTUNG UND VERFAHREN ZUM ERSTELLEN EINER ASYMMETRISCHEN PRÜFSUMME

Title (fr)

DISPOSITIF ET PROCÉDÉ POUR CRÉER UNE SOMME DE CONTRÔLE ASYMMÉTRIQUE

Publication

EP 3314768 B1 20200304 (DE)

Application

EP 16750131 A 20160729

Priority

- DE 102015217724 A 20150916
- EP 2016068151 W 20160729

Abstract (en)

[origin: WO2017045824A1] The invention relates to a device for the computer-aided creation of an asymmetric checksum by a first communication partner (200), in which a processor (211) carries out the following method steps: A first method step (105) for calculating a mapped checksum (c') by means of bijective mapping (G) from a first checksum (c1), wherein the first checksum (c1) from the set of all possible checksums (C) is assigned by means of a first function (F1) to respectively one message (m) from a set of all possible messages (M), the first checksum (c1) is prepared in particular by mapping the set of all possible checksums (C) onto a first set (CA) by a second function (F2). A second method step (110) for the distribution of information which defines an inverse function (G-1) relative to the bijective mapping (G) to at least one second communication partner (300), wherein the first checksum (c1) is calculated from the mapped checksum (c') by means of the inverse function(G-1). A third method step (115) for transmitting the mapped checksum (c') and the message (m) to the at least one second communication partner (300).

IPC 8 full level

H03M 13/09 (2006.01); **H03M 13/00** (2006.01); **H04L 9/32** (2006.01)

CPC (source: EP US)

H03M 13/09 (2013.01 - EP US); **H03M 13/096** (2013.01 - US); **H03M 13/616** (2013.01 - EP US); **H04L 9/3247** (2013.01 - US); H04L 63/123 (2013.01 - US)

Designated contracting state (EPC)

AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

DOCDB simple family (publication)

DE 102015217724 A1 20170316; CN 108141226 A 20180608; EP 3314768 A1 20180502; EP 3314768 B1 20200304; ES 2788638 T3 20201022; US 10797730 B2 20201006; US 2018241417 A1 20180823; WO 2017045824 A1 20170323

DOCDB simple family (application)

DE 102015217724 A 20150916; CN 201680053942 A 20160729; EP 16750131 A 20160729; EP 2016068151 W 20160729; ES 16750131 T 20160729; US 201615752321 A 20160729